



Overview of Public Zone Work Environments

Introduction

The Internet allows employees to remain hyperconnected and reachable any place and at any time. This flexibility provides work-life balance as employees can telework from different environments, however, it also increases the threats and presents greater security risks to the enterprise. The **Public Access Zone** implements the necessary interfaces between the internet and internal departmental network services. This Public Access Zone acts as a demilitarized zone, or buffer, from the malicious activity that prevails on the Internet. Work environments such as a residence, the Wired Internet, and Wireless Hotspots offer access channels into the enterprise network.

Work Environments

Residence

The residence work environment is more prevalent than other environments as a way for employees to conduct enterprise work related tasks from a home-based office.

Security Issues – Enterprise IT administrators have less control over the employee owned end-system with respect to the OS platform, the image used, applications installed, and host security controls. The employee-owned end-system is usually a shared device within a residence, possibly lead to unauthorized access to sensitive information by other home occupants.

Mitigation – Enterprises should use endpoint compliance solutions to ensure that end-systems accessing their private network are running the latest security patches and enabling mandatory security controls.

Wired Internet

The Wired Internet work environment is comprised of facilities where commercial or privately-owned equipment connects to the Public Zone via an Ethernet cable such as that found in hotels or Internet Cafés.

Security Issues – Commercially owned end-systems in this environment present the greatest risk to both employees and to the enterprise, as these systems may be infected and could allow unauthorized access to sensitive information.

Mitigation – Employees should use Internet Café desktops as a last resort and refrain from conducting sensitive business.

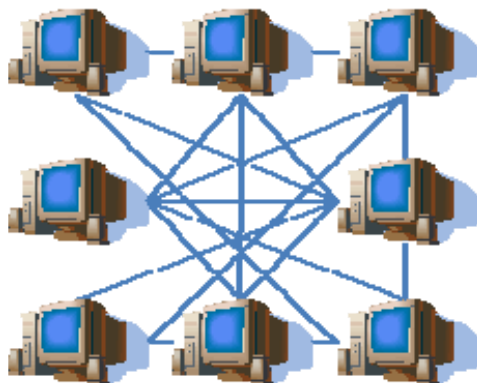


Wireless Hotspot

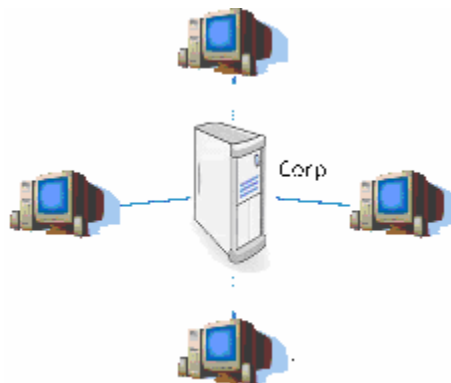
The Wireless Hotspot work environment such as those found in Airports or at business conferences provide Wi-Fi access to the Internet for employees.

Security Issues – Hotspot providers generally configure the wireless links in an unsecured mode for manageability of users. This can lead to interception of the transmission for analysis of enterprise information by eavesdroppers or to launch man-in-the-middle attacks.

Mitigation – Enterprise policy should disallow ad hoc connections and employees should connect to reputable and secure hotspots. For unsecured links, employees should use secure applications or tunnel them through a VPN.



Conceptual Peer-to-Peer Network



Conceptual Client/Server Network

STAND ALONE APPLICATIONS

aMule	Ares	BearShare	BitTorrent	Buzm
CSpace	EDonkey/Overnet	eMule	FastTrack	FileScope
Freenet	gift	Gnucleus	GNUnet	Gnutella2
iMesh	IRC	JXTA	KadNetwork	Kazza
KCeasy	KiwiAlpha	Krawler	Limewire	MLDonkey
Morpheus	Napshare	NeoEdge	P2PTV	PeerCasting
RetroShare	Shareaza	Shareaza	Tranche	Usenet
Vagaa	Windows Peer-to-Peer	WinMx	WPNP	Zultrax

STAND ALONE APPLICATIONS	
aMule	Ares
CSpace	EDonkey/Overnet
Freenet	gift
iMesh	IRC
KCeasy	KiwiAlpha
Morpheus	Napshare
RetroShare	Shareaza
Vagaa	Windows Peer-to-Peer
BearShare	BitTorrent
eMule	FastTrack
Gnucleus	GNUnet
JXTA	KadNetwork
Krawler	Limewire
NeoEdge	P2PTV
Shareaza	Tranche
WinMx	WPNP
Buzm	MLDonkey
FileScope	PeerCasting
Gnutella2	Usenet
Kazza	Zultrax